



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/089,858	08/28/2002	Jurgen Lang	ACDPA-5003 PWO	1439
23416	7590	08/22/2006	EXAMINER	
CONNOLLY BOVE LODGE & HUTZ, LLP P O BOX 2207 WILMINGTON, DE 19899			HO, THOMAS M	
			ART UNIT	PAPER NUMBER
			2132	

DATE MAILED: 08/22/2006

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary

Application No.

10/089,858

Applicant(s)

LANG ET AL.

Examiner

Thomas M. Ho

Art Unit

2134

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

- 1) ☐ Responsive to communication(s) filed on 03 July 2006.
- 2a) ☒ This action is **FINAL**. 2b) ☐ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

- 4) ☒ Claim(s) 1-4 is/are pending in the application.
- 4a) Of the above claim(s) _____ is/are withdrawn from consideration.
- 5) ☐ Claim(s) _____ is/are allowed.
- 6) ☒ Claim(s) 1-4 is/are rejected.
- 7) ☐ Claim(s) _____ is/are objected to.
- 8) ☐ Claim(s) _____ are subject to restriction and/or election requirement.


Application Papers

- 9) ☐ The specification is objected to by the Examiner.
- 10) ☐ The drawing(s) filed on _____ is/are: a) ☐ accepted or b) ☐ objected to by the Examiner.
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).
Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

- 12) ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) ☐ All b) ☐ Some * c) ☐ None of:
1. ☐ Certified copies of the priority documents have been received.
 2. ☐ Certified copies of the priority documents have been received in Application No. _____.
 3. ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.


KAMBIZ ZAND
PRIMARY EXAMINER

Attachment(s)

- 1) ☒ Notice of References Cited (PTO-892)
- 2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
- 3) ☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08)
Paper No(s)/Mail Date _____
- 4) ☐ Interview Summary (PTO-413)
Paper No(s)/Mail Date. _____
- 5) ☐ Notice of Informal Patent Application (PTO-152)
- 6) ☐ Other: _____

DETAILED ACTION

1. Claims 1-4 are pending.
2. The amendment of 7/03/06 has been received and entered.

Response to Arguments

3. In light of Applicant's amendments, the rejections under 35 USC 112 have been withdrawn.

The Applicant has argued on page 5 and 6

Examiner Ho's attention is directed to the fact that digital signatures according to the state of the art (Houser) require a huge amount of data to be transferred. This is especially disadvantageous if the size of the data is of importance. A very important field for generating smaller forgery-proof document if the size of the data is of importance. A very important field for generating smaller forgery-proof documents is the generation of digital postmarks.

In order to achieve this advantage of the invention, the security module according to claim 1 contains the characteristic that the output value of the combination machine (K2) is used to form an irreversible hash and that hash value is output from the outlet valve.

These characteristics are not found in Houser which proposes a usage of digital signature algorithms for securing data.

The Examiner contends that regardless of the advantages Applicant's invention may or may not provide, the claims must be written in such a way as to claim those particular limitations and must not be broad to the extent that it reads upon existing prior art. Although the Applicant has claimed that "*that the output value of the combination machine (K2) is used to form an irreversible hash and that hash value is output from the outlet valve*" the Examiner notes that Houser discloses the embedding of a security object, where the information of the security object may disclose a hash. (Column 4, lines 10-35) Furthermore, Applicant's disclosure of digital postmarks, while providing useful background information, does not alter the scope of the claims. Additionally, the prior art Houser also offers the use of digital watermarks as an additional digital security measure in Figure 7D, and Figure 8.

Essentially, though the Applicant may be claiming the usage of digital watermarks of irreversible hashes, it appears that Houser uses them as well. (Column 4, lines 10-35) Although Houser may use a broader invention which may include information other than digital hashes, such as additional encryption and or digital signatures, it does not render Houser any less anticipatory to digital hashes and postmarks to the extent that Applicant's claims recite them.

Claim Rejections - 35 USC § 102

4. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

A person shall be entitled to a patent unless –

(b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of application for patent in the United States.

5. Claims 1-4 are rejected under 35 U.S.C. 102(b) as being anticipated by Houser et al, US patent 5606609.

In reference to claim 1:

Houser et al. discloses a method for producing forgery-proof documents or data records using a security module,

- Whereby the security module generates a secret which remains unknown to a document producer and the document producer can not gain access to the secret which can only be encrypted by an authentication unit, where the secret is the embedded security object (Column 3, lines 50-60) & Figure 1, Item 130, and where the document producer (Figure 1, Item 110) cannot gain access to the secret in that it can only send information from the electronic document security application but not receive information from it as indicated by the flow of arrows, and where the secret is encrypted by the authentication unit, the electronic document security application.
- Whereby the secret, together with information that reveals details about the identity of the security module, is transferred in encrypted form to an authentication unit, where the authentication unit is the electronic document security application (Column 3, lines 3, line 60 – Column 4, line 17) & (Column 12, lines 40-67)
- Whereby an authentication unit decrypts the secret, recognizes the identity of the security module and encrypts the secret, together with information on the identity of the document

producer, in such a way that only a checking unit can carry out a decryption and then the authentication unit transmits these to the document producer, where the checking unit is the verification aspect of the security application (Column 4, lines 3-34)

- Whereby the document producer transfers its own data to the security module, (Figure 1, Items 110 to 130)
- Whereby the security module irreversibly links by hash encryption the secret with the data that the document producer itself has introduced, and (Column 3, lines 50-60) & (Column 13, lines 13-20) & (Column 15, lines 15-25) & (Column 4, lines 10-35)
- Whereby it is not possible to draw conclusions about the secret. (Column 4, lines 3-10)

Characterized in that the result of the irreversible linking of the secret with the data introduced by the document provider, the data introduced by the document producer itself as well as the encrypted information of the authentication unit all serve to form the document that is transmitted to the checking unit. (Column 7, lines 65- Column 8, lines 20) (Figure 1, Items 140, 150) & (Column 3, lines 50-60)

In reference to claim 2:

Houser et al. (Column 10, line 60 – Column 11, line 10) & (Column 17, lines 30-60) discloses the method according to claim 1, characterized in that the additional information transferred by the authentication unit contains details on the identity of the document producer and on the period of validity of the documents generated by the document producer.

In reference to claim 3:

Art Unit: 2134

Houser et al. (Column 3, lines 50 – Column 4, lines 10) & (Column 4, lines 11 – 34) & (Column 21, lines 20-35) & Figure 8 discloses the method for checking the authenticity of a document, characterized in that the checking unit checks whether the result of an irreversible linking by hash encryption of a secret with data introduced by a document producer have been incorporated into the document, in that the checking unit decrypts the secret and additional information that were encrypted by an authentication unit, in that the checking unit irreversibly links the decrypted secret with the data introduced into the document by the document producer, in the same manner as a security module used to produce the forgery-proof document, and in that the checking unit compares the result of the irreversible linking that it has performed itself with the result of an irreversible linking that was performed by the document producer and incorporated into the document, where the document is the document, where the irreversible linking of the secret is the embedding of the security object into the document, and where the security object hash is the signature digest (Column 4, lines 10-16) where the checking unit is the verification unit, where the verification unit decrypts the embedded security object in order to validate the document.

In reference to claim 4:

Houser et al. (Column 4, lines 19-46) discloses the method according to claim 3, characterized in that the comparison determines whether data introduced into the document by the document producer has been forged.

Conclusion

6. The following art not relied upon is made of record:
- US patent 5859911 discloses the comparison of two hashes to determine its validity
 - US patent 6023296 discloses a Cellular telephone apparatus with microprocessor performing hash calculation - derives audit hash value as result of memory contents calculation, and compares value with valid value derived from hash calculation performance on authentic memory contents
7. THIS ACTION IS MADE FINAL. Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of the final action and the advisory action is not mailed under after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension pursuant to 37 CFR 1.136(A) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of this final action.

8. Any inquiry concerning this communication from the examiner should be directed to Thomas M Ho whose telephone number is (571)272-3835. The examiner can normally be reached on M-F from 9:30 AM - 6:00 PM.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor,

Application/Control Number: 10/089,858

Page 8

Art Unit: 2134

Gilberto Barron can be reached on **(571)272-3799**.

The Examiner may also be reached through email through Thomas.Ho6@uspto.gov

Any inquiry of a general nature or relating to the status of this application or proceeding should be directed to the receptionist whose telephone number is (571)272-2100.

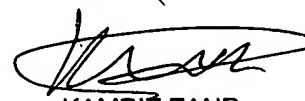
General Information/Receptionist Telephone: 571-272-2100 Fax: 571-273-8300

Customer Service Representative Telephone: 571-272-2100 Fax: 571-273-8300

TMH



August 16th, 2006



KAMBIŽ ZAND
PRIMARY EXAMINER